有限体上の楕円曲線の位数計算の最近の進展について (符号と暗号の代数的数理)

AUTHOR(S):

佐藤, 孝和

CITATION:

佐藤, 孝和. 有限体上の楕円曲線の位数計算の最近の進展について (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 32-37

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25255

数理解析研究所講究録 1361 巻 2004 年 32-37

有限体上の楕円曲線の位数計算の最近の進展について

埼玉大学・理学部数学科* 佐藤 孝和 (Takakazu Satoh)
Department of Mathematics, Saitama University*

1. はじめに

p を素数、$q:=p^m$ とし、$\mathbf{F}_q$ を位数が q の有限体とする。$E/\mathbf{F}_q$ を Weierstrass form で与えられた楕円曲線とする。ここで考えるのは「E の $\mathbf{F}_q$ 有理点の群 $E(\mathbf{F}_q)$ の位数もとめる速いアルゴリズムを設計するにはどうすればよいか」という問題である。

このような問題を考える理由はいろいろある。純粋に数論の問題として考えてもこの問題は見掛け程簡単ではなく、実際現在知られている方法で使われている道具をみればわかるように、この問題は十分挑戦しがいがある。

他の理由として、楕円曲線暗号からの要請がある。一部の弱い拡大次数を除けば楕円曲線暗号の解読されにくさは用いる楕円曲線に支配される。[1] 個々の楕円曲線 $E/\mathbf{F}_q$ に対しては $\#E(\mathbf{F}_q)$ の影響が特に大きい。このような応用においては q の bitsize[2] が 160~320 に対してパソコンでも数秒以内に $\#E(\mathbf{F}_q)$ を計算することが求められる。

楕円曲線の位数計算に関してはすでに Schoof[12], Elkies[3] あるいは拙稿 [11,13] などのいくつかの survey がでているのでここではそれらの survey が出版されたあとの進展として Lercier-Lubicz の quasi-square order アルゴリズムおよび Kohel による AGM の一般化と解釈について解説する。

以下、本稿では**簡単のため $\log\log q$ あるいは $\log m$ の項は無視する**ことにし、時間計算量は bit 演算の数で計るものとする。また計算に先立ち $\mathbf{F}_q$ は与えられているとする。すなわち、$\mathbf{F}_q\cong\mathbf{F}_p[X]/\langle f\rangle$ となる（都合の良い）$f\in\mathbf{F}_p[X]$ は既知とする。

2. 多項式時間アルゴリズム

いままで知られている $\log q$ あるいは m に関する多項式時間アルゴリズムはすべて q 乗 Frobenius 写像 Fr_q の trace を計算し、Hasse の定理：$\#E(\mathbf{F}_q)=1+q-\mathrm{Tr}(\mathrm{Fr}_q)$, $|\mathrm{Tr}(\mathrm{Fr}_q)|\leq 2\sqrt{q}$ を用いて位数を求める。$\mathrm{Tr}(\mathrm{Fr}_q)$ の計算方法には大別して二つの方法がある。

---

* 現在の所属：東京工業大学理工学研究科数学専攻
current affiliation: Department of Mathematics, Tokyo Institute of Technology

[1] 特定の m に関しては $\mathbf{F}_{p^m}$ 上の全ての楕円曲線離散対数問題に対して Weil decent attack が適用可能になってしまい、そのような体上の楕円曲線を用いた楕円暗号は同程度の q に対する楕円暗号よりも弱い (Menezes, Teske, Weng[9]). 楕円暗号を構成する際はそのような m は最初から除外しておくので位数計算が重要なことに変わりはない。

[2] $\log_2 q$ のこと

l-adic algorithm: (Schoof-Atkin-Elkies, SEA)

多くの小さい素数 l $(\neq p)$ に対して $\mathrm{Tr}(\mathrm{Fr}_q) \bmod l$ を求め、CRT を用いて $\mathrm{Tr}(\mathrm{Fr}_q)$ を復元する。時間計算量は証明されているのは $O((\log q)^5)$ だが経験則としてはほとんどの場合に $O((\log q)^4)$ である。2003 年中には目だった進展は筆者の知る限りなかったが、ただ SEA は今でも p が大きいときに使える最速のアルゴリズムであることを記しておく。

p-adic algorithm:

小さな素数 p が固定されていて $m \to \infty$ としたときの漸近的高速アルゴリズム。E を $\mathbf{Q}_p$ の不分岐 m 次拡大体上に持ち上げ $\mathrm{Tr}(\mathrm{Fr}_q) \bmod p^{m/2+O(1)}$ を計算する。これを書いている時点では $O(m^{2.5})$ が最速[3] アルゴリズムである。p 進アルゴリズムを考えているときは O-constant は p に依存することに注意する。

3. p-adic algorithm の概要

p を固定された小さな素数[4]、Kを $\mathbf{Q}_p$ の不分岐 m 次拡大体、R を K の付値環、π を適当な意味での reduction $\bmod p$ map $(R \to \mathbf{F}_q,\ \mathbf{P}^2(K) \to \mathbf{P}^2(\mathbf{F}_q),\ \ldots)$ とする。E を $j(E) \notin \mathbf{F}_{p^2}$ を満たす $\mathbf{F}_q$ 上の楕円曲線とする（特に E は ordinary である）。$E^{\uparrow}/K$ が E の **canonical lift** であるとは $\pi(E^{\uparrow}) = E$ かつ $\mathrm{End}(E^{\uparrow}) \cong \mathrm{End}(E)$ となることを言うのであった。(Lubin, Serre, Tate[8], Messing[10]) このとき

$$\begin{array}{ccc} \mathrm{Isog}(E_1, E_2) & \cong & \mathrm{Isog}(E_1^{\uparrow}, E_2^{\uparrow}) \\ \cup\!\!| & & \cup\!\!| \\ f & \to & f^{\uparrow} \end{array}$$

は Abel 群の同型を与える。Fr_q の dual isogeny を V_q と書く。p 進位数計算法では TrFr_q の代りに標数 0 の体 K 上の曲線 $E^{\uparrow}$ の endomorphism $V_q^{\uparrow}$ の trace を計算する。[5] ここで問題となるのは $E^{\uparrow}$ の Weierstrass model（あるいは j-invariant）を求めるアルゴリズムである。

Φ_p を p 次 modular 多項式、$\sigma \in \mathrm{Gal}(K/\mathbf{Q}_p)$ を Frobenius 置換[6] とする。$j(E) \notin \mathbf{F}_{p^2}$ だったので $j(E^{\uparrow})$ は

$$\begin{cases} \Phi_p(j(E^{\uparrow}), \sigma(j(E^{\uparrow}))) = 0 \\ \pi(j(E^{\uparrow})) = j(E) \end{cases}$$

として特徴付けられる。(Lubin, Serre, Tate[8]) この方程式をできるだけ効率良く解く方法を見つけ

---

[3] この主要項は数学的に単純なノルム計算に由来し、canonical lift の構成だけなら $O(m^2)$ で済む。(Harley[4])

[4] p が大きくても以下で解説するアルゴリズムは動くが m を止めて $p \to \infty$ としたときの振舞は素朴に個数を数えるのと同程度の計算量が必要となってしまう。現実的には $p < 100$ 程度が限度であろう。

[5] ただし $V_q^{\uparrow}$ を直接扱うのでは計算量が大きくなりすぎるので $V_p^{\uparrow}$ を介して TrFr_q を計算する。また Frobenius ではなくその dual を用いるのは $\mathbf{F}_q$ 上では Frobenius は inseparable だが V_p は separable であり計算機上で扱いやすいためである。

[6] $\sigma : E \to \sigma(E)$ は $\mathrm{Fr}_p^{\uparrow}$ **ではない**。実際、σ は単射だが $\mathrm{Fr}_p^{\uparrow}$ は次数が p で単射にはなり得ない。

たいのであるが：

- $R/p^{m/2+O(1)}R$ の元の四則演算の時間計算量は $O(m^2)$
- 事前計算を認めなければ σ の時間計算量は知られている限り $O(m^3)$[7]
- σ は K 上の関数として微分できない

など状況はかなり厳しい。[11] が書かれた時点での最速のアルゴリズムは事前計算無しでは時間 $O(m^3)$、領域 $O(m^2)$、体にのみ依存する事前計算を認めれば時間 $O(m^{2.5})$, 領域 $O(m^2)$ であった。これより増大度の小さなアルゴリズムを作るためには $R/p^{m/2+O(1)}R$ の演算 $o(\sqrt{m})$ 回に相当する計算しか行えないのである。

4. Lercier-Lubicz の quasi-square lifting

Lercier, Lubicz[7] は $\mathbf{F}_q/\mathbf{F}_p$ が型の小さな Gaussian Normal Base (以下 GNB) を持つとき事前計算なしで時間 $O(m^2)$ の canonical lift 構成アルゴリズムを与えた。

$t\in\mathbf{N}$ かつ $mt+1$ は p と異る素数とする。τ を $\mathbf{F}_{mt+1}$ の中の 1 の原始 t 乗根、γを $\mathbf{F}_p^a$ の中の 1 の原始 $mt+1$ 乗根とする。このとき $\theta:=\sum_{i=0}^{t-1}\gamma^{\tau^i}$ $(\in\mathbf{F}_q)$ を type (m,t) の **Gauss period** という。p の $\mathbf{F}_{mt+1}^{\times}$ における位数を e とおくと、θ が $\mathbf{F}_q/\mathbf{F}_p$ の正規底を生成するためには $\gcd(mt/e,m)=1$ が必要十分であり、これを $\mathbf{F}_q/\mathbf{F}_p$ の type t **Gaussian normal base** (GNB) というのであった。[8]
$\mathbf{F}_q/\mathbf{F}_p$ が type t の GNB $\{\theta^{p^n}\}_{n=0}^{m-1}$ を持つとき以下が成立する (Kim et al.[5]).

(1) これは $K/\mathbf{Q}_p$ の正規底 $\{\sigma^n(\Theta)\}_{n=0}^{m-1}$ $(\pi(\Theta)=\theta)$ に持ち上がる。以下、Θ として 1 の冪根をとる。
(2) $\mathbf{Q}_p$-normed vector space K の基底として $\{\sigma^n(\Theta)\}_{n=0}^{m-1}$ は正規直交基底である。[9]
(3) $\{\sigma^n(\Theta)\}_{n=0}^{m-1}$ の $\mathbf{Z}_p$ 係数一次結合により表現された R の二つの元の乗算は $\{\Theta^{n}\}_{n=0}^{m-1}$ の $\mathbf{Z}_p$ 係数一次結合により表現された R の二つの元の乗算よりもおおよそ t 倍遅い。特に t を止めれば乗算の時間計算量の漸近的増大度は同じである。
(4) $\{\sigma^n(\Theta)\}_{n=0}^{m-1}$ の $\mathbf{Z}_p$ 係数一次結合により表現された R の元の x に対して $\sigma^k(x)$ を求めるのは $O(m)$ でできる。(特にこの時間は k に依存しない。)

Lercier, Lubicz は $\mathbf{F}_q/\mathbf{F}_p$ に GNB があるとき $F(X,Y)\in R[X,Y]$ に対して $F(x,\sigma(x))=0$ の解に二乗収束する解の近似列を各項を計算する時間計算量 $O(m^2)$ で構成した。$\sigma:K\to K$ は微分できないから Newton 法はそのままでは使えない。

---

[7] ここは改善の余地があるかも知れない。

[8] 「$\mathbf{F}_q/\mathbf{F}_p$ が type 1 GNB を持つ⇔ $e=m$ ⇔ p が $\mathbf{F}_{m+1}$ の原始根」となる。原始根に関する Artin 予想が正しければ $\mathbf{F}_p$ 上 type 1 GNB を持つ拡大次数が無限個存在する。特に「漸近的増大度」が意味を持つ。

[9] 完備非アルキメデス的付値体 $(k,|\cdot|)$ 上の n 次元 normed k-vector space $(V,\|\cdot\|)$ のベクトル $v_1,\ \ldots,\ v_n\in V-\{0\}$ は任意の $a_1,\ \ldots,\ a_n\in k$ に対して $\left\|\sum_{i=1}^{n}a_iv_i\right\|=\max_{1\le i\le n}|a_i|\|v_i\|$ が成立するとき **Vの直交基底**をなすという。V の直交基底 $\{v_1,\ldots,v_n\}$ は $\|v_i\|=1$ for all $1\le i\le n$ のとき**正規直交基底**と言う。$v=\sum_{i=1}^{n}a_iv_i$ を誤差 ε まで決めることは $a_1,\ \ldots,\ a_n$ を誤差 ε まで決めることであり、局所体上の元を指定された精度まで求めなければならないときには都合の良い基底である。なお、「正規」がまったく異なる二つの意味で使われていることに注意。

$F(x_n, \sigma(x_n)) \equiv 0 \bmod p^{2^n}$, $\partial_Y F(x_n, \sigma(x_n)) \in R^\times$ となる $x_n \in R$ が与えられたとき $h \in p^{2^n}R$ を選び $x_{n+1} := x_n + h$ が $F(x_{n+1}, \sigma(x_{n+1})) \equiv 0 \bmod p^{2^{n+1}}$ を満たすようにするには h をどのように取ればよいであろうか。$A_n := \partial_X F(x_n, \sigma(x_n))$, $B_n := \partial_Y F(x_n, \sigma(x_n))$ とおくと

$$F(x_{n+1}, \sigma(x_{n+1})) = \underbrace{F(x_n, \sigma(x_n)) + A_n h + B_n \sigma(h)}_{\equiv 0 \bmod O(p^{2^{n+1}}) \text{としたい}} + O(p^{2^{n+1}})$$

となるから $\sigma(t) = -A_n B_n^{-1} t - p^{-2^n} F(x_n, \sigma(x_n)) B_n^{-1}$ の解を $\bmod p^{2^n}$ まで求めたものを h とすれば良い。

そこで一般に $a, b \in R$ とし、方程式

$$\sigma(t) = at + b \qquad (*)$$

の解 $t \in R$ を求めることを考える。一見しただけではこれが解を持つのか、持ったとしても一意的なのかどうか自明ではない。そこで Lercier-Lubicz は (*) の解を直接求めるのではなく、各 $u \in \mathbf{N}$ に対して

$$(*)\text{を満たす（任意の）}\ t \text{に対し}\ \sigma^u(t) = \sigma^u(\alpha_u)t + \sigma^u(\beta_u) \qquad (**)$$

となる α_u, $\beta_u \in R$ を構成する[10] アルゴリズムを与えた。明らかに $\alpha_1 := \sigma^{m-1}(a)$, $\beta_1 := \sigma^{m-1}(b)$ と採れる。α_u, β_u が求まったとすると

$$\sigma^{2u}(t) = \sigma^u(\sigma^u(t)) \overset{(**)}{=} \sigma^u(\sigma^u(\alpha_u)t + \sigma^u(\beta_u)) = \sigma^{2u}(\alpha_u)\sigma^u(t) + \sigma^{2u}(\beta_u)$$
$$\overset{(**)}{=} \sigma^{2u}(\alpha_u)(\sigma^u(\alpha_u)t + \sigma^u(\beta_u)) + \sigma^{2u}(\beta_u)$$

だから $\alpha_{2u} := \sigma^{2u}(\alpha_u)\sigma^u(\alpha_u)$, $\beta_{2u} := \sigma^{2u}(\alpha_u)\sigma^u(\beta_u) + \sigma^{2u}(\beta_u)$ と採れる。α_{2u+1}, β_{2u+1} についても同様な式ができる。これらを用いれば α_m, β_m が求まる。これは

$$\sigma^m(t) = \sigma^m(\alpha_m)t + \sigma^m(\beta_m)$$

を意味する。ところが α_m, β_m, $t \in R$ だから (*) の解は

$$t = \alpha_m t + \beta_m \quad \text{i.e.} \quad t = \frac{\beta_m}{1-\alpha_m}$$

を満たさねばならない。特に $\alpha_m \neq 1$ ならば (*) の解は一意的である。また $t \bmod p^\nu$ を求める時間計算量は $O(m\nu)$[11] である。これから $F(x, \sigma(x)) = 0$ の解を $\bmod p^\nu$ まで求める計算量も $O(m\nu\log\nu)$ であることが分かる。

5. Kohel による AGM の解釈

実数 $a \geq b > 0$ に対して

$$\mathcal{M}(a, b) := \left(\frac{a+b}{2}, \sqrt{ab}\right)$$

とおく。与えられた $a_0 \geq b_0 > 0$ から二つの数列 $\{a_n\}_{n=1}^\infty$ と $\{b_n\}_{n=1}^\infty$ を

$$(a_{n+1}, b_{n+1}) := \mathcal{M}(a_n, b_n)$$

により定めると良く知られているように $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$ となる。この共通の値を算術幾何平均 (arithmetic-geometric mean, AGM) という。

---

[10] α_u, β_u は一意的ではないかも知れないが (**) を満たすものをとにかく一組与える

[11] $\log m$ の項を無視しないことにすれば N bit の object の乗算の時間計算量を T_N とすると $O(T_{m\nu}\log m)$.

標数 0 の完備付値体でも a_0/b_0 が十分 1 に近ければ AGM が定義される。ここで平方根の符号は $\sqrt{ab}=a\sqrt{b/a}$ で $\sqrt{b/a}$ が 1 に近いものと定める。2001 年頃から Gaudry-Harley-Mestre はこれを標数 2 の有限体上定義された楕円曲線の位数計算に応用した。彼らの方法は $p=2$ にのみしか使えないが非常に簡素・高速である。

Input: E: $y^2+xy=x^3+u$ $(u\in\mathbf{F}_q-\mathbf{F}_4)$

Output: $\mathrm{Tr}(\mathrm{Fr}_q)$

Procedure:

1: $a:=1$; $b:=1+8$(u の R への持ち上げ) ;
2: $M:=\lfloor m/2\rfloor+3$;
3: for ($i:=0$; $i<M-2$; $i:=i+1$)
4: $\quad(a,b):=\mathcal{M}(a,b)$;
5: $(c,d):=\mathcal{M}(a,b)$;
6: return $t\in\mathbf{Z}$ s.t. $t\equiv N_{K/\mathbf{Q}_2}\left(\frac{a}{c}\right)\bmod 2^M$ and $|t|\le 2\sqrt{q}$;

もちろん、本当に速いアルゴリズムを作るためには二変数ではなく非斉次の一変数 AGM を使うなど種々の工夫が必要であるがここで考えたいのはそのような問題ではなく、「このアルゴリズムの本質はなんであろうか？」ということである。

これに対して R. Carls[2] は $A^{(0)}/R$ を ordinary reduction を持つ Abelian scheme とし、帰納的に $A^{(n)}:=A^{(n-1)}/(\pi(A^{(n-1)})[p]_{\mathrm{loc}}$ の lift) と定めると $\lim_{n\to\infty}A^{(nm)}=A^{\uparrow}$, i.e.,

$$\forall j\in\mathbf{N}\exists N\in\mathbf{N}\forall n\in\mathbf{N}[n>N\to A^{(nm)}\times W_j\cong A^{\uparrow}\times W_j]$$

(ここで $W_j:=R/p^jR$) が成立しするという定式化（と j に対して N をどのように決めるか）を与えた。また、この方針で標数 3 の有限体上の楕円曲線に対するアルゴリズムを与えた。しかし、このアルゴリズムは (少なくとも今のままでは) あまり速くはない。楕円曲線に限定しても良いから効率の良いアルゴリズムに直結する解釈が求められる。

Kohel[6] は $X_0(N)$ 上の対応という視点で AGM を一般化した。H を上半平面、$X_0(N)$ を level N の modular curve とする。

$$\begin{array}{ccccc} X_0(pN) & \to & X_0(N) & \times & X_0(N) \\ \cup & & & \cup & \\ (E,G) & \to & (\ (E,pG) & , & (E/NG,G/NG)\ ) \end{array}$$

という写像は $X_0(N)$ 上の algebraic correspondence を導く。これを定義する多項式を $\Psi_{p,N}$ とする。たとえば $X_0(1)$ の parameterization が j のときは $\Psi_{p,1}(t_1,t_2)=\Phi_p(t_1,t_2)$ となる。

上半平面内の $\mathbf{Q}$ 上二次の無理数である点 τ に対し $\delta(\tau):=B^2-4AC$ (A, B, $C\in\mathbf{Z}$, 互いに素 $A\tau^2+B\tau+C=0$) とおく。Birch[1] に従い $\bar{\tau}\in X_0(N)$ ($\bar{}$ は H の元の $X_0(N)$ における類) は $\delta(\tau)=\delta(N\tau)$ であるとき $X_0(N)$ の **Heeger point** であると定義する。

定理 (Kohel[6]) $X_0(N)$ の genus が 0 であるとする。x_1, x_2, …, x_m, $x_{m+1}=x_1\in R^{\times}$ が $\mathbf{Q}$ 上代数的、かつ $i=1\sim m$ に対して

- $\Psi_{p,N}(x_i,x_{i+1})=0$
- $x_{i+1}\equiv x_i^p \bmod p$

を満たすのなら、x_i 達は $\mathbf{Q}_p$ 上 Galois 共役で ($X_0(N)$ の parameterization を経由して) Heegner point に対応する。

これは Φ_p の代りに $\Psi_{p,N}$ を使っても canonical lift が構成できることを意味する。もし $\Psi_{p,N}$ が Φ_p よりも簡単な形になるのなら定数倍ではあるが位数計算が速くなる。定数倍というと大したことはないように聞こえるがこの“定数倍”は実際の計算では影響が大きい。たとえば

$$\Psi_{2,2}(x,y) = x^2 - 16(256y+3)xy - y$$

$$\Psi_{2,8}(x,y) = x^2(4y+1)^2 - y$$

となり $\Psi_{2,8}$ が Gaudry-Harley-Mestre の AGM に対応する。2 次の modular 多項式は

$$\Phi_2(x,y) = x^3+y^3-x^2y^2+2^4 3\cdot 31(x^2y+yx^2)-2^4 3^4 5^3(x^2+y^2)$$
$$+3^4 5^3 4027xy+3^8 3^7 5^6(x+y)-2^{12}3^4 5^9$$

だったからその差は明らかであろう。Kohel[6] では $p \geq 3$ の場合も含めていくつかの計算例が示されており、AGM の奇数標数への実用的な一般化を与えていると言えよう。また、Kohel の方法は Lercier-Lubciz の方法と組み合わせて使うことができいっそうの高速化が達成される。

References

1. Birch, B.J.: Heegner points of elliptic curves, Convegno di Strutture in Corpi Algebrici, INDAM, (Rome, 1973), Symposia Mathematica, **15**, 441-445, London: Academic Press, 1975.
2. Carls, R.: A generalized arithmetic geometric mean, (2003) preprint, available at http://www.math.leidenuniv.nl/~carls/.
3. Elkies, N.D.: Elliptic and modular curves over finite fields and related computational issues, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., **7**, 21-76, Providence, RI: AMS, 1998.
4. Harley, R.: Asymptotically optimal p-adic point counting, (2002) Post to NMBRTHRY list.
5. Kim, H., Park, J., Cheon, J., Park, J., Kim, J. and Hahn, S.: Fast elliptic curve point counting using Gaussian normal basis, Algorithmic number theory (Sydney, Australia, July 2002), Lect. Notes in Comput. Sci., **2369**, 292-307, ed. Fieker, C. and Kohel, D., Berlin: Springer, 2002.
6. Kohel, D.: The AGM-$X_0(N)$ Heegner point lifiting algorithm and elliptic curve point counting, Advances in cryptology -- ASIACRYPT 2003, Lect. Notes in Comput. Sci., **2894**, 124-136, ed. Goss, G., Hartmanis, J. and van Leeuwen, J., Berlin: Springer, 2003.
7. Lercier, R. and Lubicz, D.: Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time, Advances in cryptology - EUROCRYPT 2003, Lect. Notes in Comput. Sci., **2656**, 360-373, ed. Biham, E., Berin, Heidelberg: Springer Verlag, 2003.
8. Lubin, J., Serre, J.-P. and Tate, J.: Elliptic curves and formal groups, (1964) Mimeographed notes, available at http://www.ma.utexas.edu/users/voloch/lst.html.
9. Menezes, A., Teske, E. and Weng, A.: Weak fields for ECC, preprint, IACR archive 2003/128.
10. Messing, W.: The crystals associated to Barsotti-Tate groups: with applications to Abelian schemes. Lect. Notes in Math., 264. Berin-Heidelberg-New York: Springer 1972.
11. Satoh, T.: On p-adic point counting algorithms for elliptic curves over finite fields, Algorithmic number theory (Sydney, Australia, July 2002), Lect. Notes in Comput. Sci., **2369**, 43-66, ed. Fieker, C. and Kohel, D., Berlin: Springer, 2002.
12. Schoof, R.: Counting points on elliptic curves over finite fields. J. Théor. Nombres Bordeaux, **7**, 219-254 (1995).
13. 佐藤孝和：有限体上の楕円曲線の位数計算アルゴリズム．日本応用数理学会論文誌，**13**, 135-150 (2003).